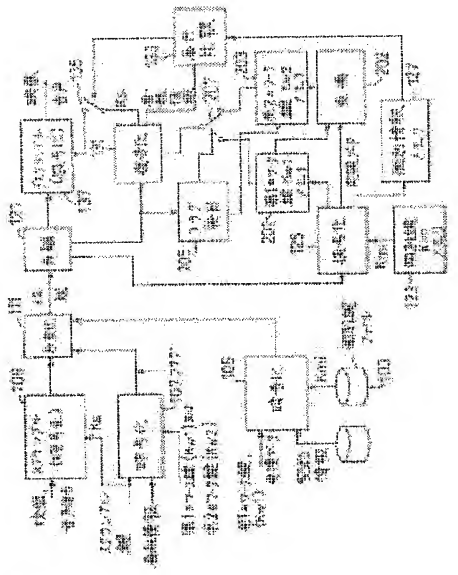
PAY BROADCAST SYSTEM AND ITS ENCODER AND DECODER

Publication number: JP9307872 (A)
Publication date: 1997-11-28
Inventor(s): OI SHINICHI
Applicant(s): TOKYO SHIBAURA ELECTRIC CO
Classification:
- international: ***H04N7/167; G06F21/24; H04H20/00; H04H60/15; H04H60/23; H04L9/08;*** **H04N7/167; G06F21/00; H04H1/00; H04L9/08;** (IPC1-7): H04N7/167; H04H1/00
- European:
Application number: JP19960117369 19960513
Priority number(s): JP19960117369 19960513

Abstract of **JP 9307872 (A)**

PROBLEM TO BE SOLVED: To reduce number of transmission times for individual information. SOLUTION: A ciphering circuit 105 ciphers a 1st substantial work key and conversion data. As a key of a ciphering circuit 107, the 1st work key or a 2nd work key obtained by converting the 1st work key with conversion data is used. A decoding circuit 125 recovers the 1st work key and the conversion data. A conversion circuit 202 converts the 1st work key by the conversion data to generate a 2nd work key. A decoding circuit 131 uses the 1st or 23nd work key corresponding to the ciphered key of the ciphering circuit 107.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－307872

(43)公開日　平成９年(1997)11月28日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｎ　7/167			Ｈ０４Ｎ　7/167	Ｚ	
Ｈ０４Ｈ　1/00			Ｈ０４Ｈ　1/00	Ｆ	

審査請求　未請求　請求項の数15　ＯＬ　（全８頁）

(21)出願番号　特願平8－117369

(22)出願日　平成８年(1996)５月13日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　大井　伸一
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝マルチメディア技術研究所内

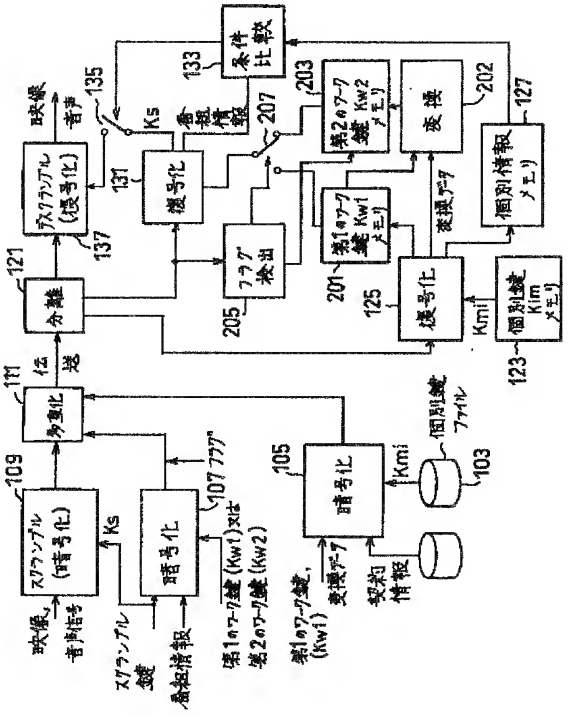
(74)代理人　弁理士　大胡　典夫

(54)【発明の名称】　有料放送方式並びにそのエンコーダとデコーダ

(57)【要約】

【課題】　個別情報の伝送回数を削減する。

【解決手段】　暗号化回路１０５で本来の第１のワーク鍵と変換データを暗号化する。暗号化回路１０７の鍵として、第１のワーク鍵またはこの鍵を前記変換データで変換された第２のワーク鍵を使用する。復号化回路１２５は、第１のワーク鍵と前記変換データを再生する。変換回路２０２は、前記変換データにより第１のワーク鍵を変換し第２のワーク鍵を生成する。復号化回路１３１は、暗号化回路１０７の暗号鍵に対応して第１または第２のワーク鍵を使用する。



1

【特許請求の範囲】

【請求項１】　少なくとも３層の暗号構造を有する有料放送において、

第３の層の第１の鍵により個別情報、第２層の第２の鍵、前記第２の鍵の変換データを暗号化する第１の暗号化手段と、

前記第２の鍵または前記第２の鍵を前記変換データにより変換して得られた第３の鍵により番組情報とスクランブル鍵を暗号化する第２の暗号化手段と、

前記第１の復号化手段の出力を前記第１の鍵により復号し、前記個別情報、前記第２の鍵、前記変換データを再生する第１の復号化手段と、

前記第２の鍵を記憶する第１の記憶手段と、

前記第１の記憶手段からの前記第２の鍵を前記変換データにより変換して前記第３の鍵を生成する変換手段と、

前記変換手段からの前記第３の鍵を記憶する第２の記憶手段と、

前記第１の記憶手段からの前記第２の鍵または前記第２の記憶手段からの前記第３の鍵により、前記第２の暗号化手段の出力を復号し、前記番組情報と前記スクランブル鍵を再生する第２の復号手段と、

を具備したことを特徴とする有料放送方式。

【請求項２】　前記変換データは、前記第２の鍵の各ビットの順序の入れ替え方のデータであることを特徴とする請求項１記載の有料放送方式。

【請求項３】　前記変換データは、前記第２の鍵のデータの回転方向と回転量を示すデータであることを特徴とする請求項１記載の有料放送方式。

【請求項４】　前記変換データは、前記第２の鍵のビット順序の反転を指示するデータであることを特徴とする請求項１記載の有料放送方式。

【請求項５】　前記変換データは、前記第２の鍵への加算データであることを特徴とする請求項１記載の有料放送方式。

【請求項６】少なくとも３層の暗号構造を有するエンコーダにおいて、

第３の層の第１の鍵により個別情報、第２層の第２の鍵、前記第２の鍵の変換データを暗号化する第１の暗号化手段と、

前記第２の鍵または前記第２の鍵を前記変換データにより変換して得られた第３の鍵により番組情報とスクランブル鍵を暗号化する第２の暗号化手段と、

を具備したことを特徴とするエンコーダ。

【請求項７】　前記変換データは、前記第２の鍵の各ビットの順序の入れ替え方のデータであることを特徴とする請求項６記載のエンコーダ。

【請求項８】　前記変換データは、前記第２の鍵のデータの回転方向と回転量を示すデータであることを特徴とする請求項６記載のエンコーダ。

【請求項９】　前記変換データは、前記第２の鍵のビット順序の反転を指示するデータであることを特徴とする請求項６記載のエンコーダ。

2

【請求項１０】　前記変換データは、前記第２の鍵への加算データであることを特徴とする請求項６記載のエンコーダ。

【請求項１１】　少なくとも３層の暗号構造を有し、

第３の層の第１の鍵により個別情報、第２層の第２の鍵、前記第２の鍵の変換データを暗号化する第１の暗号化手段と、

前記第２の鍵または前記第２の鍵を前記変換データにより変換して得られた第３の鍵により番組情報とスクランブル鍵を暗号化する第２の暗号化手段と、

を具備したエンコーダから伝送されてくる放送を受信するデコーダにおいて、

前記第１の復号化手段の出力を前記第１の鍵により復号し、前記個別情報、前記第２の鍵、前記変換データを再生する第１の復号化手段と、

前記第２の鍵を記憶する第１の記憶手段と、

前記第１の記憶手段からの前記第２の鍵を前記変換データにより変換して前記第３の鍵を生成する変換手段と、

前記変換手段からの前記第３の鍵を記憶する第２の記憶手段と、

前記第１の記憶手段からの前記第２の鍵または前記第２の記憶手段からの前記第３の鍵により、前記第２の暗号化手段の出力を復号し、前記番組情報と前記スクランブル鍵を再生する第２の復号手段と、

を具備したことを特徴とするデコーダ。

【請求項１２】　前記変換データは、前記第２の鍵の各ビットの順序の入れ替え方のデータであることを特徴とする請求項１１記載のデコーダ。

【請求項１３】　前記変換データは、前記第２の鍵のデータの回転方向と回転量を示すデータであることを特徴とする請求項１１記載のデコーダ。

【請求項１４】　前記変換データは、前記第２の鍵のビット順序の反転を指示するデータであることを特徴とする請求項１１記載のデコーダ。

【請求項１５】　前記変換データは、前記第２の鍵への加算データであることを特徴とする請求項１１記載のデコーダ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、有料放送方式並びにそのエンコーダとデコーダに関する。

【０００２】

【従来の技術】有料放送では、契約した者のみが放送を享受できるように、映像及び音声信号にスクランブルを施し放送を行っている。

【０００３】このスクランブルを解除する処理は、大きく分けて２つある。１つは、映像及び音声信号にかけられたスクランブルを解除し、元の信号に戻す処理であ

る。もう１つは、そのデスクランブルがスクランブルを解除しても良いか否かの判断を行う処理つまり放送局との契約状態を条件比較して判断し、デスクランブル処理のＯＮ／ＯＦＦを管理する処理の２つである。

【０００４】この契約管理処理では、放送局から送られてくる情報を使用するが、その情報には暗号がかけられており、契約した者のデコーダのみが情報を取り込めるようになっている。

【０００５】図８に従来の有料放送システムの構成を示す。図示したように暗号化するデータは、階層構造になっている。

【０００６】暗号化回路１０５には、暗号化されるものとして、放送局から各デコーダへの個別の契約情報（以下、個別情報という）とワーク鍵Ｋｗが供給されている。前記個別情報は、契約した者のデコーダが視聴できるようにするための情報である。暗号化回路１０５には、また個別鍵ファイル１０３から個別鍵Ｋｍｉ（ｉは、個別鍵がデコーダごとに異なることを示すためにつけた）が供給されている。暗号化回路１０５は、個別鍵Ｋｍｉにより個別情報とワーク鍵Ｋｗを暗号化する。

【０００７】このため、その個別鍵を有しないデコーダでは、その暗号化されている情報を取り込むことができず、他人の情報を只見するような不正ができないようになっている。ただし、当然のことながら個別鍵は個々に異なるため、例えば１０万台のデコーダを制御するためには、この個別情報を１０万個送出する必要があるというように、個々のデコーダに対し情報を送る必要があり、管理するデコーダ数が増えると送るデータ量も多くなり大変である。

【０００８】また、ワーク鍵Ｋｗは、後述する番組情報を不正に利用されないように暗号化するための鍵である。暗号方式自体の解析がしにくいように、ワーク鍵Ｋｗは定期的に変更することが必要であるとされている。

【０００９】これは、例えば暗号化された番組情報とその復号結果の一部である後述するスクランブル鍵Ｋｓとの関係から、ワーク鍵Ｋｗや暗号方式そのものの解析をされる危険性があるので、その危険を低くするために、ワーク鍵Ｋｗを変更するという考えによっている。

【００１０】このため、例えば月に１度とかあるいは年に１度というタイミングでワーク鍵Ｋｗを更新するように、放送局からデコーダに対してワーク鍵Ｋｗを含む個別情報を与えるようになっている。

【００１１】暗号化回路１０７には、暗号化されるものとして、各デコーダに共通に与える番組に関する情報（以下、番組情報という）とスクランブル鍵Ｋｓが供給される。暗号化回路１０７は、ワーク鍵Ｋｗによって番組情報とスクランブル鍵Ｋｓを暗号化する。

【００１２】スクランブル回路１０９には、暗号化されるものとして映像、音声信号が供給される。スクランブル回路１０９は、スクランブル鍵Ｋｓによって映像、音

声信号を暗号化する。

【００１３】多重化回路１１１は、暗号化回路１０５、暗号化回路１０７、スクランブル回路１０９からの信号を多重する。多重化された信号は、デコーダ側に伝送される。

【００１４】分離回路１２１は、入力を分離し、暗号化回路１０５の出力信号を復号化回路１２５に、暗号化回路１０７の出力信号を復号化回路１３１に、スクランブル回路１０９の出力信号をデスクランブル回路１３７に供給する。

【００１５】復号化回路１２５は、個別鍵Ｋｍｉメモリ１２３からの個別鍵Ｋｍｉにより暗号化回路１０５の出力信号を復号し、個別情報とワーク鍵Ｋｗを再生する。個別情報は、個別情報メモリ１２７に記憶され、ワーク鍵Ｋｗは、ワーク鍵Ｋｗメモリ１２９に記憶される。

【００１６】復号化回路１３１は、ワーク鍵Ｋｗメモリ１２９からのワーク鍵Ｋｗにより暗号化回路１０７の出力信号を復号し、番組情報とスクランブル鍵Ｋｓを再生する。スクランブル鍵Ｋｓは、スイッチ１３５に供給される。

【００１７】条件比較回路１３３は、個別情報メモリ１２７からの個別情報と復号化回路１３１からの番組情報を比較し、視聴可能であればスイッチ１３５をＯＮにする。その結果、スクランブル鍵Ｋｓが、デスクランブル回路１３７に供給される。

【００１８】デスクランブル回路１３７は、スクランブル鍵Ｋｓによりスクランブル回路１０９の出力信号を復号し、映像、音声信号を再生する。

【００１９】

【発明が解決しようとする課題】上述したように、個別鍵Ｋｍｉはデコーダごとに異なるため、ワーク鍵Ｋｗを更新し個々のデコーダへ与えるためには台数分の個別情報を送出しなければならない。しかし、デコーダ数が増えてくると、個別情報を送付するデータ量が膨大になり、データを送付するチャンネル容量を大きくするかあるいは全てのデコーダを制御するまでに必要な時間を長くとるなどの措置をとる必要があった。

【００２０】そこで本発明は、ワーク鍵を更新するたびに個別情報を送る必要の無い有料放送方式並びにそのエンコーダとデコーダを提供することを目的とする。

【００２１】

【課題を解決するための手段】

（有料放送方式）少なくとも３層の暗号構造を有する有料放送において、第３の層の第１の鍵により個別情報、第２層の第２の鍵、前記第２の鍵の変換データを暗号化する第１の暗号化手段と、前記第２の鍵または前記第２の鍵を前記変換データにより変換して得られた第３の鍵により番組情報とスクランブル鍵を暗号化する第２の暗号化手段と、前記第１の復号化手段の出力を前記第１の鍵により復号し、前記個別情報、前記第２の鍵、前記変

換データを再生する第１の復号化手段と、前記第２の鍵を記憶する第１の記憶手段と、前記第１の記憶手段からの前記第２の鍵を前記変換データにより変換して前記第３の鍵を生成する変換手段と、前記変換手段からの前記第３の鍵を記憶する第２の記憶手段と、前記第１の記憶手段からの前記第２の鍵または前記第２の記憶手段からの前記第３の鍵により、前記第２の暗号化手段の出力を復号し、前記番組情報と前記スクランブル鍵を再生する第２の復号手段と、を具備したことを特徴とする。

【００２２】（エンコーダ）少なくとも３層の暗号構造を有するエンコーダにおいて、第３の層の第１の鍵により個別情報、第２層の第２の鍵、前記第２の鍵の変換データを暗号化する第１の暗号化手段と、前記第２の鍵または前記第２の鍵を前記変換データにより変換して得られた第３の鍵により番組情報とスクランブル鍵を暗号化する第２の暗号化手段と、を具備したことを特徴とする。

【００２３】（デコーダ）少なくとも３層の暗号構造を有し、第３の層の第１の鍵により個別情報、第２層の第２の鍵、前記第２の鍵の変換データを暗号化する第１の暗号化手段と、前記第２の鍵または前記第２の鍵を前記変換データにより変換して得られた第３の鍵により番組情報とスクランブル鍵を暗号化する第２の暗号化手段と、を具備したエンコーダから伝送されてくる放送を受信するデコーダにおいて、前記第１の復号化手段の出力を前記第１の鍵により復号し、前記個別情報、前記第２の鍵、前記変換データを再生する第１の復号化手段と、前記第２の鍵を記憶する第１の記憶手段と、前記第１の記憶手段からの前記第２の鍵を前記変換データにより変換して前記第３の鍵を生成する変換手段と、前記変換手段からの前記第３の鍵を記憶する第２の記憶手段と、前記第１の記憶手段からの前記第２の鍵または前記第２の記憶手段からの前記第３の鍵により、前記第２の暗号化手段の出力を復号し、前記番組情報と前記スクランブル鍵を再生する第２の復号手段と、を具備したことを特徴とする。

【００２４】

【発明の実施の形態】図１に、本発明の有料放送方式の実施の形態の構成を示す。従来例と同じ動作をする回路については、同一参照番号を付し説明は省略する。

【００２５】暗号化回路１０５には、個別情報（契約情報）、本来のワーク鍵である第１のワーク鍵Ｋｗ１とこの第１のワーク鍵Ｋｗ１を変換する変換データが供給される。前記変換データは、将来の第１のワーク鍵Ｋｗ１の変換を先取りするためのものである。暗号化回路１０５は、個別鍵Ｋｍｉにより個別情報、第１のワーク鍵、変換データを暗号化する。この暗号化されたデータ列を、図２に示す。

【００２６】暗号化回路１０７に、スクランブル鍵Ｋｓと番組情報が供給される。暗号化回路１０７は、スクランブル鍵Ｋｓと番組情報を、第１のワーク鍵Ｋｗ１又は第２のワーク鍵Ｋｗ２により暗号化する。

【００２７】第２のワーク鍵Ｋｗ２は、第１のワーク鍵Ｋｗ１を前記変換データで変換したものである。前記変換データの例とこの変換データによって生成された第２のワーク鍵Ｋｗ２の例を以下に説明する。

【００２８】前記変換データの第１の例は、第１のワーク鍵Ｋｗ１の各ビットの順序の入れ替え方のデータである。この場合の変換例を、図４に示す。前記変換データの第２の例は、第１のワーク鍵Ｋｗ１のデータの回転方向と回転量を示すデータである。例えば、右まわりに２ビット分回転させる。この場合の変換例を、図５に示す。前記変換データの第３の例は、第１のワーク鍵Ｋｗ１のビット順序の反転を指示するデータである。この場合の変換例を、図６に示す。前記変換データの第４の例は、第１のワーク鍵Ｋｗ１の各ビットに加算を指示し、その加算するデータである。この場合の変換例を、図７に示す。尚、暗号化回路１０５でおくる変換データは、一種類に限らず、複数送ることも考えられる。

【００２９】暗号化回路１０７の出力において、フラグが挿入される。フラグは、暗号化回路１０７において、どのワーク鍵を使用したかのデータと変換データの種類のデータである。

【００３０】フラグを含む暗号化された番組情報、スクランブル鍵Ｋｓのデータ列を、図３に示す。

【００３１】復号化回路１２５は、個別鍵Ｋｍｉにより復号化を行い、個別情報、第１のワーク鍵Ｋｗ１、前記変換データを出力する。第１のワーク鍵Ｋｗ１は、第１のワーク鍵Ｋｗ１メモリ２０１に供給される。前記変換データは、変換回路２０２に供給される。変換回路２０２には、また第１のワーク鍵Ｋｗ１メモリ２０１から第１のワーク鍵Ｋｗ１が供給される。変換回路２０２は、上述したように前記変換データにより第１のワーク鍵Ｋｗ１を変換して、第２のワーク鍵Ｋｗ２を生成し、第２のワーク鍵Ｋｗ２メモリ２０３に供給する。各メモリ２０１、２０３からの第１と第２のワーク鍵Ｋｗ１とＫｗ２が、スイッチ２０７に供給されている。

【００３２】フラグ検出回路２０５は、フラグを検出し、暗号化回路１０７で使用したワーク鍵がどちらであるかを検出する。フラグ検出回路２０５は、第１のワーク鍵Ｋｗ１が使用された場合は、スイッチ２０７を第１のワーク鍵Ｋｗ１メモリ２０１側に倒し、第２のワーク鍵Ｋｗ２が使用された場合は、スイッチ２０７を第２のワーク鍵Ｋｗ２メモリ２０３側に倒す。フラグ検出回路２０５は、またどの変換データが使用されたかを検出し、第２のワーク鍵Ｋｗ２メモリから読み出す第２のワーク鍵Ｋｗ２の種類を選択する。

【００３３】復号化回路１３１は、スイッチ２０７で選択されたワーク鍵により復号して、番組情報とスクランブル鍵Ｋｓを出力する。

7

【００３４】変換データとしては、複数の変換方法を組み合わせものであっても良い。例えば、図４に示す変換をした後、図５に示す変換をしても良い。

【００３５】変換データが一種類の場合、エンコーダ側でのフラグの挿入をやめると共に、フラグ検出回路２０５を省略する。この場合、復号化回路１３１は、第１と第２のワーク鍵Ｋｗ１とＫｗ２を順次選択し合致するものを使用する。

【００３６】また、グループ個別情報では、そのグループに含まれるデコーダに対するワーク鍵だけでなく、契約情報（グループ個別情報）も与えることになるため、ワーク鍵を更新させたくないデコーダを除いて契約情報を与えることができず不便であったが、本発明では契約情報に関しては、既にデコーダに蓄積されているものをそのまま使用するのでそのような不便さがなく、ワーク鍵を変更できる。

【００３７】

【発明の効果】上述したように、本発明では個別情報に本来の第１のワーク鍵Ｋｗ１を変換するデータをあらかじめ１つ以上いれておき、番組情報の復号時に、第１のワーク鍵Ｋｗ１を前記変換データで変換し使用するので、ワーク鍵を変更するためだけに個別情報を送らなくても良く、伝送チャンネルの有効利用をはかることができる。

【図面の簡単な説明】

8

【図１】本発明の有料放送システムの実施の形態の構成を示す図である。

【図２】暗号化された個別情報のデータ列を示す図である。

【図３】暗号化された番組情報、スクランブル鍵Ｋｓのデータ列を示す図である。

【図４】本来の第１のワーク鍵Ｋｗ１の変換例を示す図である。

【図５】本来の第１のワーク鍵Ｋｗ１の変換例を示す図である。

【図６】本来の第１のワーク鍵Ｋｗ１の変換例を示す図である。

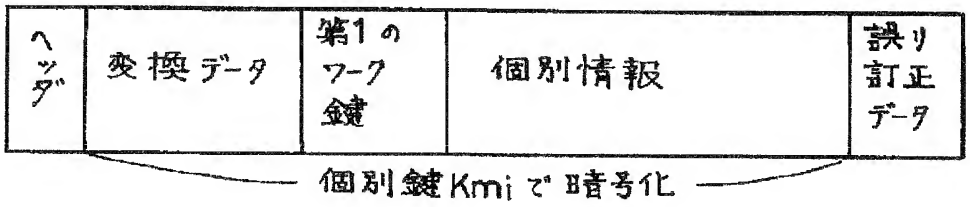
【図７】本来の第１のワーク鍵Ｋｗ１の変換例を示す図である。

【図８】従来の有料放送方式の構成を示す図である。

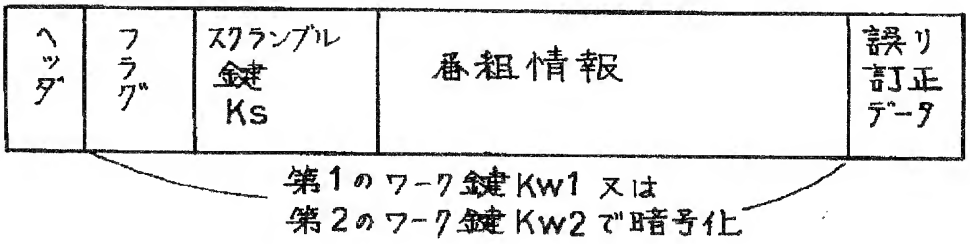
【符号の説明】

１０３・・・個別鍵ファイル、１０５、１０７・・・暗号化回路、１０９・・・スクランブル回路、１１１・・・多重化回路、１２１・・・分離回路、１２３・・・個別鍵Ｋｍｉメモリ、１２５・・・復号化回路、１２７・・・個別情報メモリ、１３１・・・復号化回路、１３３・・・条件比較回路、１３５・・・スイッチ、１３７・・・デスクランブル回路、２０１・・・第１のワーク鍵Ｋｗ１メモリ、２０２・・・変換回路、２０３・・・第２のワーク鍵Ｋｗ２メモリ、２０７・・・スイッチ。

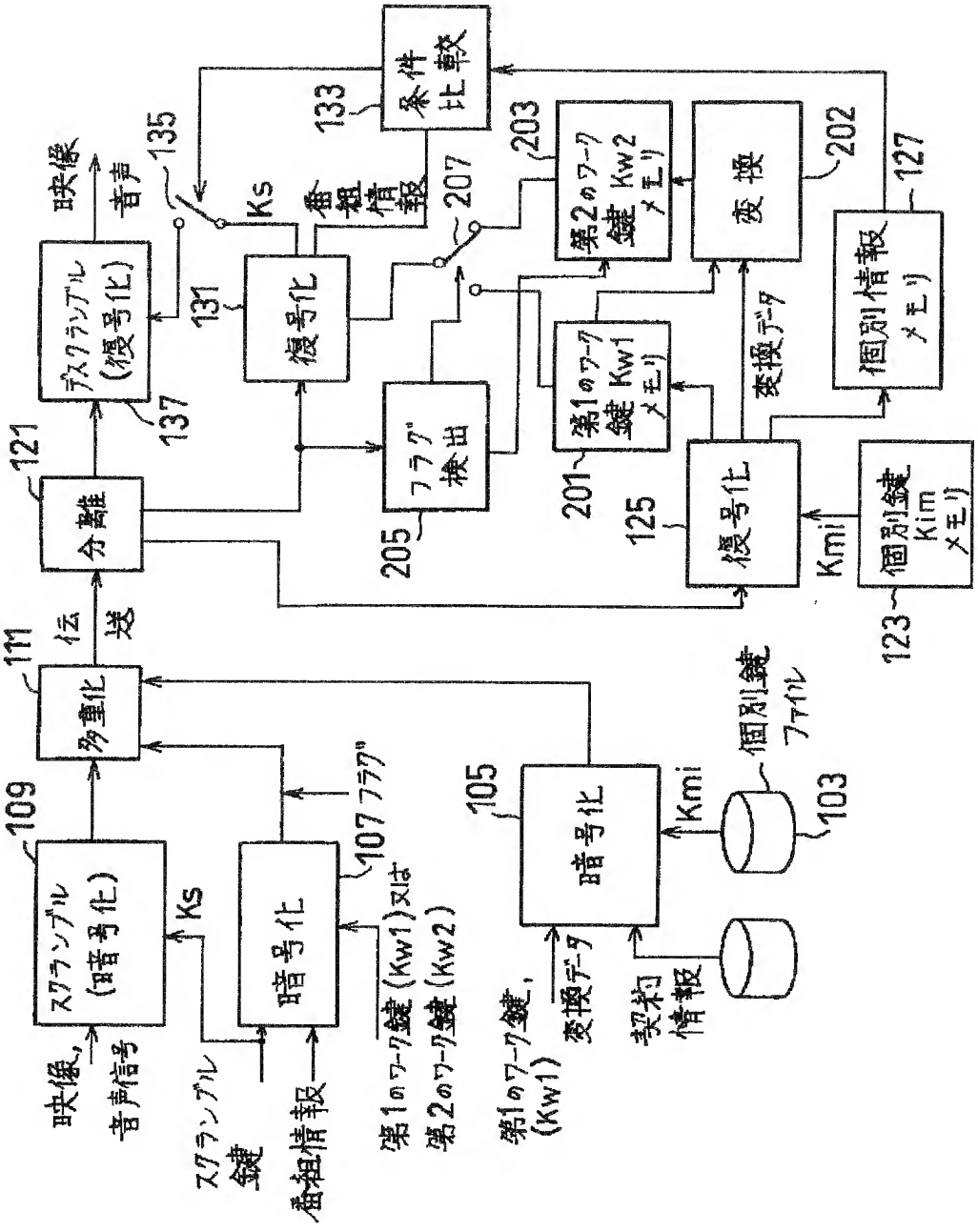
【図２】



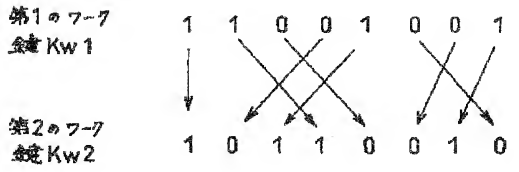
【図３】



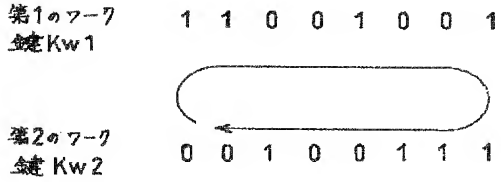
【図１】


映像，音声信号
スクランブル鍵
番組情報
第1のワード鍵 (Kw1)又は第2のワード鍵 (Kw2)
第1のワード鍵，(Kw1)
変換データ
契約情報
スクランブル (暗号化)
暗号化
多重化
伝送
分離
デスクランブル (復号化)
復号化
フラグ検出
条件比較
暗号化
復号化
変換
第1のワード鍵 Kw1 メモリ
第2のワード鍵 Kw2 メモリ
個別情報メモリ
個別鍵 Kim メモリ
個別鍵ファイル
Ks
Kmi
フラグ
109
111
121
131
133
135
137
105
107
103
201
203
205
207
202
125
127
123

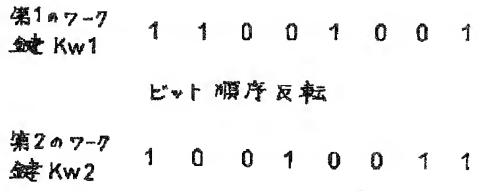
【図４】


第1のワーク
鍵 Kw1
1 1 0 0 1 0 0 1
第2のワーク
鍵 Kw2
1 0 1 1 0 0 1 0

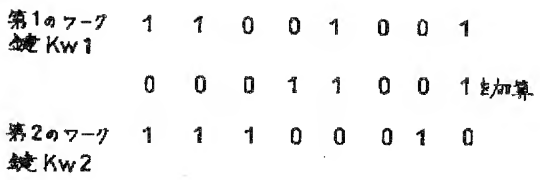
【図５】


第1のワーク
鍵 Kw1
1 1 0 0 1 0 0 1
第2のワーク
鍵 Kw2
0 0 1 0 0 1 1 1

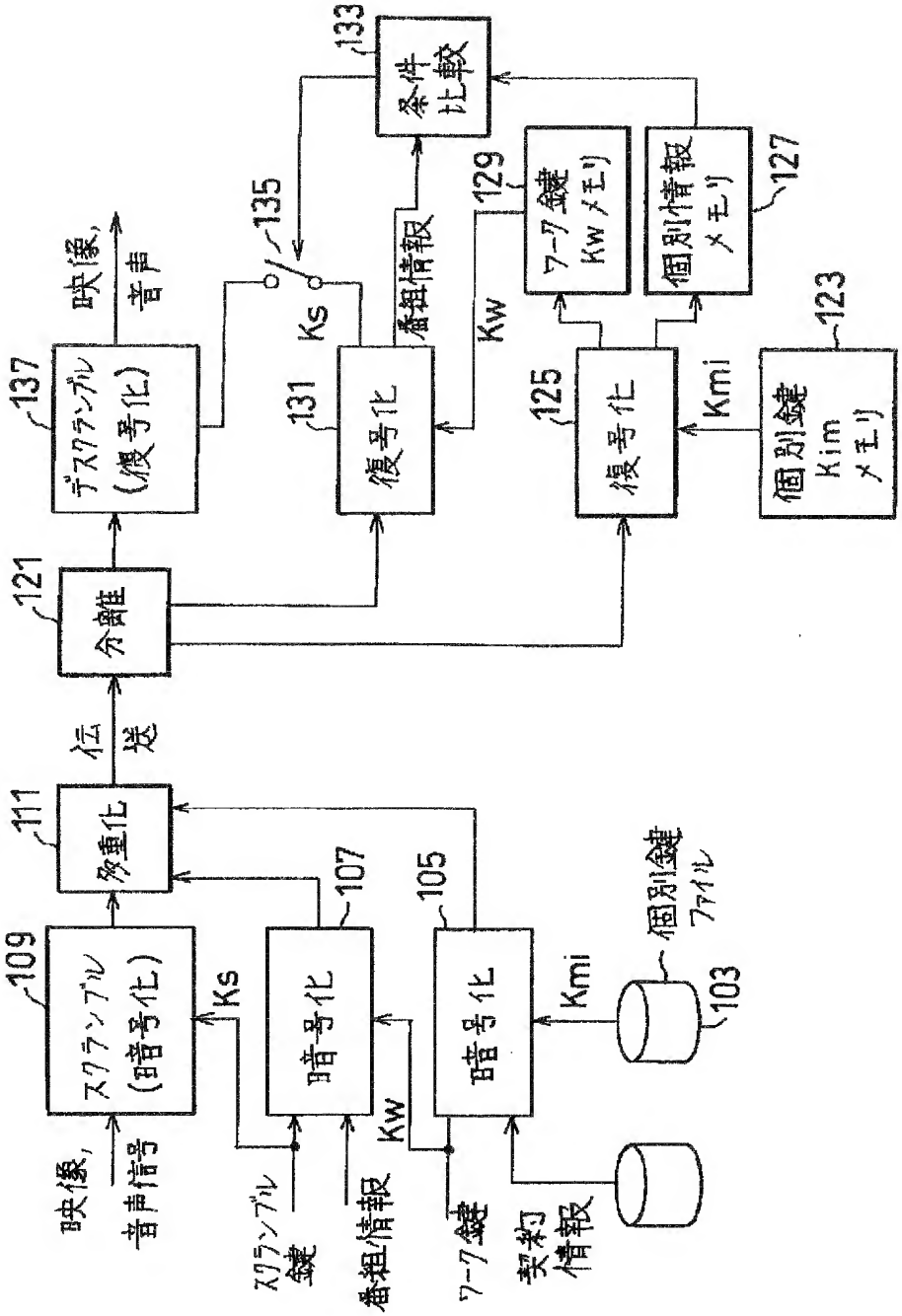
【図６】


第1のワーク
鍵 Kw1
1 1 0 0 1 0 0 1
ビット 順序 反転
第2のワーク
鍵 Kw2
1 0 0 1 0 0 1 1

【図７】


第1のワーク
鍵 Kw1
1 1 0 0 1 0 0 1
0 0 0 1 1 0 0 1 を加算
第2のワーク
鍵 Kw2
1 1 1 0 0 0 1 0

【図８】


映像，
音声信号
スクランブル
(暗号化)
109
Ks
多重化
111
伝送
暗号化
107
暗号化
105
Kmi
個別鍵
ファイル
103
スクランブル
鍵
番組情報
KW
ワーク鍵
契約
情報
分離
121
デスクランブル
(復号化)
137
映像，
音声
復号化
131
Ks
135
番組情報
条件
比較
133
Kw
ワーク鍵
Kwメモリ
129
個別情報
メモリ
127
復号化
125
Kmi
個別鍵
Kim
メモリ
123